DASHLANE

Credential Security as a Regulatory Imperative

Credential security has moved from best practice to regulatory mandate. Financial services organizations face a tightening band of credential security requirements. Regulators across the U.S., EU, and UK are translating long-standing best practices into prescriptive technical mandates: 12-character passwords under PCI DSS 4.0.1, mandatory MFA for essential entities under NIS2, strong authentication for critical functions under DORA, and material incident disclosure under SEC cybersecurity rules. The expectations are converging, and the audit evidence required to meet them is moving from periodic snapshots to continuous, workforce-wide visibility.

Yet most financial institutions are running their compliance programs on top of credential security architectures that were not built for this bar.

4 gaps stand between today's controls and tomorrow's audit

1 Access gap

SSO leaves a critical chunk of financial services applications uncovered, including legacy core banking and trading systems, vendor and partner portals, specialty compliance tools, and the shadow SaaS that examiners increasingly flag as a material control weakness.

2 Adoption gap

Vault-based password managers protect only what employees actively store. Coverage plateaus well before full workforce adoption, leaving a material segment of users—and the unmanaged credentials they handle—outside any policy enforcement.

3 Visibility gap

Email security, EDR, and SIEM tools see credential risk only after credentials are used. The browser, where financial services employees actually log in to non-SSO platforms—from clearing and settlement systems to compliance vendors to offshore operations tools—remains unmonitored.

4 Response gap

Manual remediation creates a dangerous lag between detection and action. DORA, SEC cybersecurity rules, and FFIEC examiners increasingly want evidence of timely response, not just detection.

DASHLANE

Key regulations with credential security mandates

Regulation	Credential security relevance
GDPR (Article 32)	Requires “appropriate technical and organizational measures” to secure personal data. Supervisory authorities and EDPB guidance treat weak authentication and missing MFA as Article 32 failures, with Article 5①(f) reinforcing integrity and confidentiality obligations.
HIPAA Security Rule	45 CFR § 164.308 and § 164.312 mandate Unique User Identification and Person or Entity Authentication. The January 2025 NPRM proposes making MFA explicitly required for all systems handling ePHI, removing the prior “addressable” loophole.
PCI DSS 4.0	Mandatory since 31 March 2025. Requirement 8 prescribes 12-character passwords, MFA for all access into the cardholder data environment, strong cryptographic protection of authentication factors, and full account lifecycle controls.
SOX (Section 404)	IT General Controls tested under PCAOB AS 2201 routinely cover password policy, MFA, account provisioning, and privileged access. PCAOB inspections regularly cite credential-related ITGC deficiencies as material weaknesses in ICFR.
NIST SP 800-53 / CMMC 2.0	The IA (Identification and Authentication) control family governs identification, MFA for privileged and non-privileged accounts (IA-2), and authenticator management (IA-5). Widely adopted by FS firms via NIST CSF and FFIEC examinations.
ISO/IEC 27001:2022	Annex A.5.15–A.5.18 govern access control, identity management, authentication information, and access rights. A.8.5 (Secure Authentication) reinforces strong-authentication requirements across the ISMS.
DORA (EU 2022/2554)	In force since 17 January 2025. Article 9④(c) mandates least-privilege access; Article 9④(d) requires strong authentication mechanisms for all financial entities, including banks, insurers, investment firms, and crypto-asset providers.
NIS2 (EU 2022/2555)	Article 21②(j) explicitly requires “multi-factor authentication or continuous authentication solutions”. Banks and financial market infrastructures are designated essential entities. Penalties up to €10M or 2% of global turnover.
UK Cyber Security and Resilience Bill	Introduced 12 November 2025; expected Royal Assent in 2026 with phased implementation through 2028. Designed to align UK regulation with NIS2 and codify NCSC Cyber Assessment Framework Principle B2 (Identity and Access Control).

DASHLANE

The cost of getting it wrong runs well beyond fines

Internal costs: audit drag and operational burden

Weak credential controls don't just create regulatory risk; they create a permanent operational tax. Every audit cycle becomes an evidence-collection scramble: Without continuous visibility into credential health across the workforce, IT and compliance teams default to manual screenshots, spreadsheet exports, and ad-hoc attestations that auditors challenge and examiners discount. The principle of least privilege, a baseline expectation under DORA Article 9④(c), NIST 800-53 AC-6, and ISO 27001 A.5.15, becomes nearly impossible to demonstrate when a meaningful share of credentials live outside the password management vault and outside SSO.

The trajectory is steep. Between 2016 and 2023, employee hours dedicated to financial regulation compliance and examiner mandates grew 61%, three times the rate of overall employee hours growth. Bank IT budgets devoted to compliance rose from 9.6% to 13.4% of total IT spend, and 42% of C-suite time and 43% of board time is now consumed by regulatory and supervisory compliance (Bank Policy Institute, 2024). Examiner findings drive remediation projects that compete with strategic initiatives. Cyber insurance underwriters now require evidence of credential controls before binding coverage, and they price weak controls accordingly.

External costs: fines, disclosures, and reputational damage

Direct regulatory penalties are no longer hypothetical. NIS2 authorizes fines up to €10M or 2% of global turnover for essential entities. HIPAA penalties can reach $1.5M per violation category per year. GDPR can cost up to 4% of global revenue. PCI DSS card-brand fines and DORA supervisory penalties stack on top of the rest.

But the higher external cost is increasingly public exposure. SEC cybersecurity disclosure rules require material incident reporting on Form 8-K within four business days. DORA mandates major ICT incident notification to competent authorities. Each disclosure converts a private control failure into a public event that affects share price, customer retention, and counterparty trust. A credential breach traced to a non-SSO vendor portal or an unrotated shared service account becomes an examiner case study, an analyst talking point, and a competitive disadvantage.

The flipside is just as real. Strong credential security pays back across the operational stack with faster audits, lower incident response costs, reduced cyber insurance premiums, and the freedom to expand cloud usage, third-party access, and remote work without proportionally expanding compliance risk.

DASHLANE

How Dashlane Omnix™ simplifies financial services compliance

Dashlane Omnix is the proactive credential security platform that closes the four gaps regulators are now scrutinizing to help simplify both internal audits and regulatory compliance.

Closes the access gap by securing workforce access in real time. Omnix protects credentials outside SSO across every application employees use, from core banking systems to specialty SaaS to shadow IT, and enables secure credential sharing across teams.

Closes the adoption gap by protecting every login on day one—without employee effort. Omnix delivers credential risk detection, real-time alerting, and workforce-wide insights from the moment Omnix is deployed. No waiting for vault adoption to plateau before compliance evidence becomes available.

Closes the visibility gap with beyond-the-vault visibility and audit evidence. Omnix provides organizations with continuous, workforce-wide credential health monitoring across every employee login, regardless of vault usage. This expanded visibility gives you the audit-ready reporting that PCI DSS 4.0.1, SOX, GLBA, DORA, and NIS2 increasingly require.

Closes the response gap with credential telemetry and simplified reporting. AI-powered detections feed credential threat data into existing SIEM and SOAR stacks, producing instant, audit-ready reports that shrink detection-to-remediation cycles.

The result: stronger controls, cleaner audits, and reduced regulatory exposure, without adding to the workload of already-stretched IT and security teams.

Dive deeper into Dashlane's best-in-class security.
Learn more